IN THE CLAIMS

1. (Currently amended) A data processing apparatus for ~~initially~~ generating a verifying value for verifying an individual contents data to be stored in a memory device, ~~then~~ storing said verified value in said memory device in correspondence with said contents data, and ~~finally~~ checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value, comprising: ~~; wherein~~

~~said verifying value is independently generated and stored in said memory device per category of contents data~~

a ciphering unit for generating said verifying value; and

one or more keys for use by said ciphering unit to generate said verifying value;

whereby said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device.

2. (Currently amended) The data processing apparatus according to Claim 1, wherein

said data processing apparatus is operable to compute an updated verifying value for one of said categories of contents data and compare said updated verifying value to the corresponding previously generated verifying value to determine whether or not there has been any tampering with the contents data corresponding to said category ~~computes a verifying value based on data of the objective contents data, then compares the computed verifying value to a previously stored verifying value, and finally utilizes the corresponding contents data solely in the case in which both values are identified to be coincident with each other in case of utilizing the contents data~~.

3. (Currently amended) The data processing apparatus according to Claim 1, wherein

said plurality of categories respectively correspond ~~memory device stores such contents data of a variety of categories corresponding~~ to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plurality of directories.

4. (Currently amended) The data processing apparatus according to Claim 1, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in ~~such~~ a domain preset as a utilization inhibited block in said flash memory.

5. (Canceled)

6. (Currently Amended) The data processing apparatus according to Claim 1, wherein

said categories are preset and each corresponds to a node in a hierarchical structure of categories ~~individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to a specific device; and~~

~~said categories individually preset and store such verifying values being independent from each other per controlling entity of said enabling key block~~.

7. (Currently Amended) The data processing apparatus according to Claim 1, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to a partial data message constituting a contents related data ~~such as contents data and header data respectively~~ to be subject to verification via said verifying values.

8. (Currently amended) A data processing apparatus which generates and stores message authentication codes functioning themselves as the data for probing the act of tampering with contents data or header data stored in a memory device, comprising:

a ciphering unit for generating a verifying value; and

one or more keys for use by said ciphering unit to generate one or more message authentication codes on which said verifying value is based;

whereby said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device

~~; wherein~~

~~said data processing apparatus generates a plurality of message authentication codes in such mutually different data domains in contents data or header data;~~

~~part of said data domains for generating said message authentication codes therein is utilized as a common data; and~~

~~whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well~~.

9. (Currently amended) A data processing method, comprising the steps of:

~~for initially~~ generating a verifying value for each category of a plurality of categories of contents data stored in a memory device, each said verifying value to be used for verifying an individual contents data ~~to be~~ stored in ~~a~~ said memory device,

~~then~~ storing each said ~~verified value~~ verifying values in said memory device in correspondence with a respective one of said individual contents data, and

~~finally~~ checking for the ~~to probe~~ actual occurrence ~~or absence~~ of an ~~the~~ act of tampering with said contents data by referring to one or more of said verifying values

~~; wherein~~

~~said verifying value is independently generated and stored in said memory device per category of contents data~~.

10. (Currently amended) The data processing method according to Claim 9, wherein said step of checking comprises the steps of computing an updated verifying value for one of said categories of contents data and comparing said updated verifying value to the corresponding previously generated verifying value to determine whether or not there has been any tampering with the contents data corresponding to said category ~~wherein~~

~~said data processing method computes a verifying value based on data of the objective contents data, then compares the computed verifying value to a previously stored verifying value, and finally utilizes the corresponding contents data solely in the case in which both values are identified to be coincident with each other in case of utilizing the contents data~~.

11. (Currently amended) The data processing method according to Claim 9, wherein

said plurality of categories respectively correspond ~~memory device stores such contents data of a variety of categories corresponding~~ to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plurality of directories.

12. (Currently amended) The data processing method according to Claim 9, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in ~~such~~ a domain preset as a utilization inhibited block in said flash memory.

13. (Canceled)

14. (Currently amended) The data processing method according to Claim 9, wherein

said categories are preset and each corresponds to a node in a hierarchical structure of categories ~~individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to a specific device; and~~

~~said categories individually preset and store such verifying values being independent from each other per controlling entity of said enabling key block~~.

15. (Currently amended) The data processing method according to Claim 9, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to a partial data message constituting a contents related data ~~such as contents data and header data respectively~~ to be subject to verification via said verifying values.

16. (Currently amended) The data processing method according to Claim 15, wherein said step of generating a verifying value includes generating one or more message authentication codes on which said verifying value is based

~~said contents data and header data subject to verification individually contain a plurality of message authentication codes generated in different data domains;~~

~~part of said data domains for generating said message authentication codes therein is utilized as a common data; and~~

~~whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well~~.

17. (Currently amended) A data processing method which generates and stores message authentication codes functioning ~~themselves~~ as ~~the~~ data for probing for an ~~the~~ act of

tampering with contents data or header data stored in a memory device, comprising the steps of:

performing ciphering according to one or more keys to generate said message authentication codes; and

using said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device; and

using said verifying values for probing for an act of tampering with the contents data or header data stored in the memory device

~~; wherein~~

~~said data processing apparatus generates a plurality of message authentication codes in such mutually different data domains in contents data or header data;~~

~~part of said data domains for generating said message authentication codes therein is utilized as a common data; and~~

~~whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well~~.

18. (Currently amended) A recording medium recorded with a computer program executable by a computer for performing a data processing method, the method comprising the steps of:

generating a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data stored in said memory device,

storing said verifying values in said memory device in correspondence with said contents data, and

checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to one or more of said verifying values

~~operable to store verifying values for verifying contents data in a memory device in correspondence with individual contents data and to provide a computer system with the computer program~~

~~for probing actual occurrence or absence of the act of tampering with contents data on a computer system; wherein~~

~~said computer program comprises a step of generating and storing such verifying values being independent per category of contents data~~.

19. (Currently amended) A data processing apparatus comprising:

a memory device; and

a device for (a) ~~initially~~ generating a verifying value for verifying an individual contents data to be stored in the memory device, (b) storing the verifying ~~verified~~ value in the memory device in correspondence with the individual contents data, and (c) checking for the ~~to probe actual~~ occurrence ~~or absence~~ of ~~the~~ an act of tampering with said individual contents data by referring to said verifying value;

wherein said processing apparatus is operable to generate a verifying value for each category of a plurality of categories of contents data stored in the memory device ~~said verifying value is independently generated and stored in said memory device in association with a category of the contents data~~.

20. (Previously presented) The data processing apparatus of claim 19, wherein the device computes the verifying value based on data from the individual contents data and then compares the computed verifying value to a previously stored verifying value, and finally utilizes the individual contents data solely in the case in which both values are identified to be coincident with each other.

21. (Currently amended) The data processing apparatus of claim 19, wherein said plurality of categories respectively correspond ~~the memory device stores contents data of a variety of categories corresponding~~ to a plurality of directories; and wherein the verifying value is generated to

deal with an assemblage of contents data individually corresponding to the plurality of directories.

22. (Previously presented) The data processing apparatus of claim 19, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

23. (Canceled)

24. (Currently amended) The data processing apparatus of claim 19, wherein ~~a~~ said plurality of categories are preset and each corresponds to a node in a hierarchical structure of categories ~~of contents data are individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to the device; and wherein a plurality of verifying values are independently generated and stored in the memory device in association with each of the plurality of categories of contents data~~.

25. (Previously presented) The data processing apparatus of claim 19, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

26. (Currently amended) A data processing apparatus comprising:

a memory device for storing contents data; and

a device for (a) generating and storing message authentication codes functioning ~~themselves~~ as ~~the~~ data for probing for an act of tampering with the stored contents data, (b) generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and (c) renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes;

whereby said processing apparatus is operable to use one or more of said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in said memory device.

27. (Currently amended) A method for use in a data processing apparatus, the method comprising the steps of:

initially generating a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data ~~to be~~ stored in ~~a~~ said memory device;

storing the ~~verified~~ verifying value in the memory device in correspondence with the contents data; and

checking to probe for the ~~actual~~ occurrence ~~or absence~~ of ~~the~~ an act of tampering with said contents data by referring to said verifying value~~,~~

~~wherein said verifying value is independently generated and stored in said memory device in association with a category of the contents data~~.

28. (Previously presented) The method of claim 27, further comprising the steps of:

computing the verifying value based on data from the individual contents data; and

comparing the computed verifying value to a previously stored verifying value;

using the individual contents data solely in the case in which both values are identified to be coincident with each other.

29. (Currently amended) The method of claim 27, wherein said plurality of categories respectively correspond ~~the~~

~~memory device performs the step of storing contents data of a variety of categories corresponding~~ to a plurality of directories; and wherein the verifying value is generated to deal with an assemblage of contents data individually corresponding to the plurality of directories.

30. (Previously presented) The method of claim 27, wherein the memory device comprises a flash memory; and the verifying value associated with the category is stored in a domain preset as a utilization inhibited block in said flash memory.

31. (Canceled)

32. (Currently Amended) The method of claim 27, wherein ~~a~~ said plurality of categories are preset and each corresponds to a node in a hierarchical structure of categories ~~of contents data are individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to the data processing apparatus; and wherein a plurality of verifying values are independently generated and stored in the memory device in association with each of the plurality of categories of contents data~~.

33. (Previously presented) The method of claim 27, wherein the verifying value is individually generated based on a message authentication code, which is generated by applying a Data Encryption Standard to a partial data message comprising data to be subject to verification via said verifying value.

34. (Previously presented) The method of claim 27 further comprising the steps of:

generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes.

35. (Currently amended) A method for use in a data processing apparatus, the method comprising the steps of:

generating a plurality of message authentication codes from different data domains, wherein part of the data domains used for generating said message authentication codes therein comprise common data; and

renewing the common data whenever renewing any of the plural message authentication codes for use in renewing other message authentication codes; and

using one or more of said message authentication codes to generate a verifying value for each category of a plurality of categories of contents data stored in a memory of said processing apparatus;

wherein said verifying values are used in an operation that provides an indication of whether or not there has been tampering with said contents data.

36. (Currently amended) A computer-readable medium for storing computer-executable software code, the code comprising:

code for initially generating a verifying value for each category of a plurality of categories of contents data stored in a memory device, each verifying value to be used for verifying an individual contents data to be stored in ~~a~~ said memory device;

code for storing the ~~verified~~ verifying value in the memory device in correspondence with the contents data; and

code for checking to probe for the ~~actual~~ occurrence ~~or absence~~ of ~~the~~ an act of tampering with said contents data by referring to said verifying value~~,~~

~~wherein said verifying value is independently generated and stored in said memory device in association with a category of the contents data~~.